(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－338295
（P2001－338295A）
(43)公開日　平成13年12月７日(2001.12.7)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｇ０６Ｔ　7/00	５１０	Ｇ０６Ｔ　7/00	５１０Ｂ	５Ｂ０３５
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｖ	５Ｂ０４３
19/10		Ｈ０４Ｎ　7/18	Ｋ	５Ｂ０５８
Ｇ１０Ｌ　17/00		Ｇ０６Ｋ　19/00	Ｓ	５Ｃ０５４
15/00		Ｇ１０Ｌ　3/00	５４５Ｆ	５Ｄ０１５

審査請求　未請求　請求項の数14　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願2000－156427(P2000－156427)

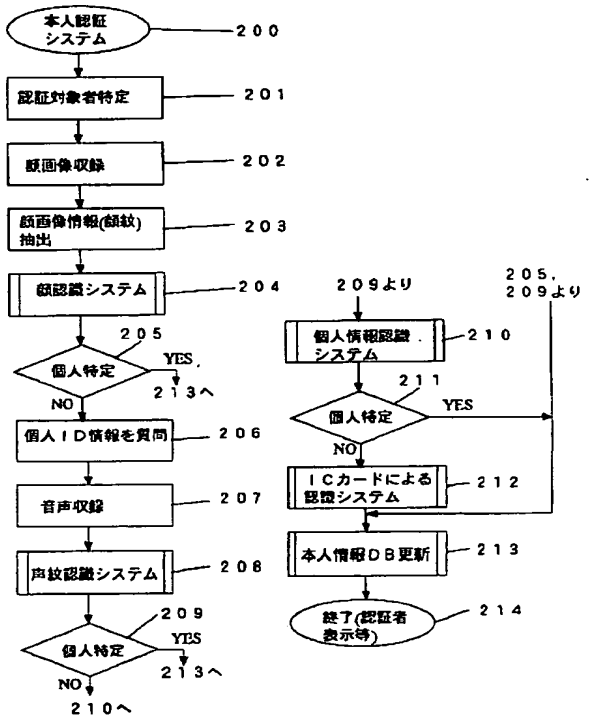
(22)出願日　平成12年５月26日(2000.5.26)

(71)出願人　500242063
ウエンズネットワーク株式会社
東京都豊島区西巣鴨１丁目２番５号
(72)発明者　伊藤　茂
東京都豊島区西巣鴨１丁目２番５号ウエンズネットワーク株式会社内
(72)発明者　大野　勝久
愛知県名古屋市昭和区御器所町名古屋工業大学内
(74)代理人　100095267
弁理士　小島　高城郎　（外１名）

最終頁に続く

(54)【発明の名称】　生態情報による本人認証システム

(57)【要約】
【課題】　認証対象者が意識することなく生態情報を利用して本人確認が実行され、かつ低コストで認証対象者、管理者、運営者に優しい、容易に実行できるシステムを提供する。
【解決手段】　認証対象者が正当な者であるか否かを生態情報を利用して判定する本人認証システムが、予め顔紋情報等の登録対象者に関する情報をデータベースに登録し、認証を実行する際にＩＣカードを有する認証対象者の顔画像を収録し顔紋情報を抽出してＩＣカード内の識別標識に該当する登録対象者の顔紋情報との適合率を、さらに音声から声紋を抽出して声紋情報との適合率を評価し個人特定する。加えて、これらの適合率を掛け合わせて評価し、さらに個人ＩＤ情報、ＩＣカード内容との一致を併せて評価することにより個人特定する。途中で特定された場合は、以降のステップを省略する。



【特許請求の範囲】

【請求項１】　施設等の入口または出口を通過しようとする認証対象者が正当な者であるか否かを認証対象者の生態情報を利用して判定する本人認証システムにおいて、

個人ＩＤ情報、顔紋情報及び声紋情報を含む登録対象者に関する情報を予め登録した登録データベースを構築し、

前記認証対象者を認証する際に、該認証対象者の顔画像を収録しその顔画像から顔紋情報を抽出し、

前記抽出された顔紋情報と、前記登録データベースに登録された全ての顔紋情報とを比較しその適合率を算出し、前記適合率が顔紋情報に係る閾値以上である登録対象者が一人のみの場合に前記認証対象者が該登録対象者であると判定し、

前記顔紋情報の適合率が、前記顔紋情報に係る閾値以上である登録対象者が零または複数である場合、前記認証対象者が自己の個人ＩＤ情報を発声した音声から声紋情報を抽出し、

前記抽出された声紋情報と前記登録データベースに登録された前記声紋情報とを比較しその適合率を算出し、前記適合率が声紋情報に係る閾値以上である登録対象者が一人のみの場合に前記認証対象者が該登録対象者であると判定し、

前記声紋情報の適合率が、前記声紋情報に係る閾値以上である登録対象者が零または複数である場合、前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせ、前記掛け合わせた数値が第１の閾値以上である登録対象者が一人のみの場合に前記認証対象者が該登録対象者であると判定することを特徴とする生態情報による本人認証システム。

【請求項２】　前記掛け合わされた数値が前記第１の閾値以上である登録対象者が零または複数である場合において、前記認証対象者が発声した自己の個人ＩＤ情報と前記登録データベースに登録されている個人ＩＤ情報とが一致する登録対象者が一人であり、かつ該登録対象者について前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第２の閾値以上であるとき、前記認証対象者を該登録対象者であると判定することを特徴とする請求項１に記載の生態情報による本人認証システム。

【請求項３】　施設等の入口または出口を通過しようとする認証対象者が正当な者であるか否かを認証対象者の生態情報を利用して判定する本人認証システムにおいて、

個人ＩＤ情報、顔紋情報及び声紋情報を含む登録対象者に関する情報を予め登録した登録データベースを構築し、

前記個人ＩＤ情報のうち少なくとも登録対象者固有の識別標識を含む前記登録対象者に関する情報を記憶したＩＣカードを予め発行し、

前記認証対象者を認証する際に、該認証対象者の顔画像を収録しその顔画像から顔紋情報を抽出すると共に、前記認証対象者が保持する前記ＩＣカードから前記識別標識を読み取り、

前記読み取った識別標識を用いて前記登録データベース内の該当する登録対象者の情報へアクセスし、

前記アクセスした登録対象者の顔紋情報と前記認証対象者の顔紋情報とを比較しその適合率を算出し、該適合率が顔紋情報に係る閾値以上である場合は、該認証対象者が該登録対象者であると判定し、

前記適合率が顔紋情報に係る閾値に達しない場合は、前記認証対象者が自己の個人ＩＤ情報を発声した音声から声紋情報を抽出し、

前記認証対象者の声紋情報と、前記読み取った識別標識に該当する前記登録対象者の声紋情報とを比較しその適合率を算出し、該声紋情報の適合率が声紋情報に係る閾値以上である場合は、前記認証対象者が該登録対象者であると判定し、前記声紋情報の適合率が声紋情報に係る閾値に達しない場合は、前記顔紋情報の適合率と前記声紋情報に係る適合率とを掛け合わせ、前記掛け合わせた数値が第１の閾値以上である場合は、前記認証対象者が前記登録対象者であると判定することを特徴とする生態情報による本人認証システム。

【請求項４】　前記掛け合わせた数値が前記第１の閾値に達しない場合において、前記認証対象者が発声した自己の個人ＩＤ情報と、前記読み取った識別標識に該当する前記登録対象者の個人ＩＤ情報とが一致し、かつ、前記登録対象者について前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第２の閾値以上であるときは、前記認証対象者が前記登録対象者であると判定することを特徴とする請求項３に記載の生態情報による本人認証システム。

【請求項５】　前記掛け合わせた数値が前記第１の閾値に達しない場合において、前記認証対象者が発声した自己の個人ＩＤ情報と、前記読み取った識別標識に該当する前記登録対象者の個人ＩＤ情報とが一致するが、前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第２の閾値に達しないとき、

前記認証対象者の前記ＩＣカードに記憶された暗証番号を読み取り、該読み取られた暗証番号と前記認証対象者が入力した暗証番号とが一致し、かつ、前記登録対象者について前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第３の閾値以上であるときは、前記認証対象者を前記登録対象者であると判定することを特徴とする請求項３に記載の生態情報による本人認証システム。

【請求項６】　前記認証対象者が前記登録対象者であると判定されたとき、前記収録された顔画像から抽出された新たな顔紋情報を前記登録データベース内の該登録対

象者に関する情報として追加登録し、追加登録された顔紋情報のデータ数が所定数を超える場合は、その中から最も古い顔紋情報を削除し、
前記認証対象者の顔紋情報と特定の登録対象者の顔紋情報とを比較しその適合率を算出する際に、該特定の登録対象者に係る全ての登録された顔紋情報と比較し、最も高い適合率を該特定の登録対象者についての前記顔紋情報の適合率とすることを特徴とする請求項１乃至５のいずれかに記載の生態情報による本人認証システム。

【請求項７】　前記認証対象者が前記登録対象者であると判定されたとき、該認証対象者が発声した音声から抽出された声紋情報を前記登録データベース内の該登録対象者に関する情報として新たに追加登録し、追加登録された声紋情報のデータ数が所定数を超える場合は、その中から最も古い声紋情報を削除し、前記認証対象者の声紋情報と特定の登録対象者の声紋情報とを比較しその適合率を算出する際に、該特定の登録対象者に係る全ての登録された声紋情報と比較し、最も高い適合率を該特定の登録対象者についての前記声紋情報の適合率とすることを特徴とする請求項１乃至５のいずれかに記載の生態情報による本人認証システム。

【請求項８】　施設等の入口または出口を通過しようとする認証対象者が本人であるか否かを該認証対象者の生態情報を利用して判定する本人認証システムにおいて、
個人ＩＤ情報、顔紋情報及び声紋情報を含む情報を記憶したＩＣカードを予め発行し、
前記認証対象者を認証する際に、該認証対象者の保持するＩＣカードに記憶された情報を読み取り、
前記認証対象者の顔画像を収録しその顔画像から顔紋情報を抽出し、
前記抽出された顔紋情報と前記ＩＣカードから読み取った顔紋情報とを比較しその適合率を算出し、前記適合率が顔紋情報に係る閾値以上である場合に前記認証対象者が本人であると判定し、
前記顔紋情報の適合率が前記顔紋情報に係る閾値に達しない場合、前記認証対象者が自己の個人ＩＤ情報を発声した音声から声紋情報を抽出し、
前記抽出された声紋情報と前記ＩＣカードから読み取った声紋情報とを比較しその適合率を算出し、前記適合率が声紋情報に係る閾値以上である場合に前記認証対象者が本人であると判定し、
前記声紋情報の適合率が、前記声紋情報に係る閾値に達しない場合、前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせ、
前記掛け合わせた数値が第１の閾値以上である場合に前記認証対象者を本人であると判定することを特徴とする生態情報による本人認証システム。

【請求項９】　前記掛け合わされた数値が前記第１の閾値に達しない場合において、前記認証対象者が発声した自己の個人ＩＤ情報と前記ＩＣカードから読み取った個人ＩＤ情報とが一致し、かつ前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第２の閾値以上である場合に前記認証対象者を本人であると判定することを特徴とする請求項８に記載の生態情報による本人認証システム。

【請求項１０】　前記掛け合わされた数値が前記第１の閾値に達しない場合において、前記認証対象者が発声した自己の個人ＩＤ情報と前記ＩＣカードから読み取った個人ＩＤ情報とが一致するが、前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第２の閾値に達しないとき、前記認証対象者のＩＣカードの暗証番号を読み取り、該読み取られた暗証番号と前記認証対象者が入力した暗証番号とが一致し、かつ、前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第３の閾値以上である場合に前記認証対象者を本人であると判定することを特徴とする請求項８に記載の生態情報による本人認証システム。

【請求項１１】　前記施設等の内部に滞在している人を管理する在籍管理システムを設け、
前記施設等へ入場する際に入場者が本人であると判定された場合に前記在籍管理システムに対してその入場の情報を渡し、かつ、該入場者が退場する際に本人であると判定された場合に該在籍管理システムに対してその退場の情報を渡すことを特徴とする請求項１乃至１０のいずれかに記載の生態情報による本人認証システム。

【請求項１２】　施設等の入口または出口を通過しようとする認証対象者が正当な者であるか否かを該認証対象者の生態情報を利用して判定する本人認証システムにおいて、
顔紋情報を含む登録対象者に関する情報を予め登録した登録データベースを構築し、
前記認証対象者を認証する際に、ビデオカメラにより撮影された映像から該認証対象者の顔画像を収録しその顔画像から顔紋情報を抽出し、
前記抽出された顔紋情報と前記登録データベースに登録された前記顔紋情報とを比較しその適合率を算出し、前記適合率が顔紋情報に係る閾値以上である登録対象者が一人のみの場合に前記認証対象者が該登録対象者であると判定し、
前記ビデオカメラにより撮影された映像上の前記認識対象者の顔画像に重ねて認証済みを示す標識を付し、
前記適合率が前記顔紋情報に係る閾値に達しない場合には、前記ビデオカメラにより撮影された映像上の前記認識対象者の顔画像に重ねて認証不可を示す標識を付すことを特徴とする生態情報による本人認証システム。

【請求項１３】　前記認証済みを示す標識が、前記登録データベースから取得した前記認証対象者の氏名であることを特徴とする請求項１２に記載の生態情報による本人認証システム。

【請求項１４】　前記認証不可を示す標識が、前記認証

対象者の顔画像をブリンキングさせることであることを特徴とする請求項１２または１３に記載の生態情報による本人認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、セキュリティ保持または安全管理を必要とする施設等への立入りまたは退去の際に、入場者若しくは退場者の本人確認を実行する認証システム、自宅などにも取り付けて簡単にセキュリティ管理を行える本人認証システム、あるいは、授業出席など人手をかけて管理している分野の効率化のために導入する本人認証システムに関する。

【０００２】

【従来の技術】ビルやオフィス、工場、研究所、マンション、病院、大学等のセキュリティ保持を必要とする施設または厳格な安全管理を必要とする施設では、入退場者がこれらの施設内に立ち入る資格をもった人間であるか否かを確認することが重要である。

【０００３】かつては、守衛の記憶に頼って本人確認を行っていた時代もあるが、近年、一般的に行われている方法の一つは、施設の出入口にいる守衛またはガードマンが入場者の提示した社員証等の身分証明書を見て、記載された事項を読むと共に身分証明書に貼付された写真と入場者の顔を見比べて本人であることを確認する方法である。しかし、多数の人を厳密にチェックすることは難しく、顔パスに近く、退職した人の入場チェックなどは不可能に近い。また、24時間複数人の監視体制を取っているが運営費用がかさんでいる。

【０００４】また、人件費節約やチェックの強化の方法としては、コンピュータ若しくは機械により読み取り可能な記録手段を具備した身分証明書を用い、コンピュータ等の読み取り装置に読み取らせる方法もある。この場合、コンピュータ等は身分証明書が正規のものであるか否かをチェックするのみであり、他人の身分証明書を携帯してなりすます入退場者には、対応することができない。また、無人であるために、正当な入退場者が入場する際に、他の人間が一緒に入退場することも可能である。さらに、近年社会環境の悪化に伴い一般家庭や事務所・学校などあらゆるところの安全管理の重要性が叫ばれており、簡便で確実な入退場者チェックシステムの出現が待たれている。

【０００５】

【発明が解決しようとする課題】上記のような方法では、高度の保安管理が要求される施設の本人認証システムとしては不十分である。完全にしようとすれば膨大な仕組みになる。そこで、例えば、指紋を利用して本人を認証するシステムを開発し、実用化の提案をしたが、指紋を採ることに抵抗を感じる人もあり、また、入退場者は、指紋を採るために手を清潔にしておく必要があり、かつフリーハンドの状態でなければならないので荷物を持っている場合などは不便である。従事する職業によっては、指紋が薄く採りにくい人もいる。指紋以外にも、生態情報すなわち顔、目、声紋等を利用した本人認証システムが提案されているが、それぞれの方式の認証率はそれほど高くなく、実用に適さないものがほとんどである。ガードマンが入退場者を個別に徹底的にチェックすることは、やはり入退場者に不快感を与えることとなる。

【０００６】以上の現状に鑑み、本発明の目的は、本人確認をされる認証対象者に不快感を与えることなく、最適には対象者が全く意識することなく、本人確認が実行されるようなシステムを提供することである。さらに、そのようなシステムであって、導入及び維持管理が容易かつ安価であり、極力無人で実行できるシステムを提供することである。

【０００７】

【課題を解決するための手段】上記の目的を達成するべく、本発明は以下の構成の本人認証システムを提供する。

（１）施設等の入口または出口を通過しようとする認証対象者が正当な者であるか否かを認証対象者の生態情報を利用して判定する本人認証システムにおいて、先ず、個人ＩＤ情報、顔紋情報及び声紋情報を含む登録対象者に関する情報を予め登録した登録データベースを構築する。そして前記認証対象者を認証する際に、該認証対象者の顔画像を収録しその顔画像から顔紋情報を抽出し、前記抽出された顔紋情報と、前記登録データベースに登録された全ての顔紋情報とを比較しその適合率を算出し、前記適合率が顔紋情報に係る閾値以上である登録対象者が一人のみの場合に前記認証対象者が該登録対象者であると判定する。さらに、前記顔紋情報の適合率が、前記顔紋情報に係る閾値以上である登録対象者が零または複数である場合、前記認証対象者が自己の個人ＩＤ情報を発声した音声から声紋情報を抽出し、前記抽出された声紋情報と前記登録データベースに登録された前記声紋情報とを比較しその適合率を算出し、前記適合率が声紋情報に係る閾値以上である登録対象者が一人のみの場合に前記認証対象者が該登録対象者であると判定する。さらに、前記声紋情報の適合率が、前記声紋情報に係る閾値以上である登録対象者が零または複数である場合、前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせ、前記掛け合わせた数値が第１の閾値以上である登録対象者が一人のみの場合に前記認証対象者が該登録対象者であると判定する。

【０００８】（２）上記（１）の構成において、前記掛け合わされた数値が前記第１の閾値以上である登録対象者が零または複数である場合には、前記認証対象者が発声した自己の個人ＩＤ情報と前記登録データベースに登録されている個人ＩＤ情報とが一致する登録対象者が一人であり、かつ該登録対象者について前記顔紋情報に係

る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第２の閾値以上であるとき、前記認証対象者を該登録対象者であると判定する。

【０００９】（３）本発明の生態情報による本人認証システムの別の構成においては、先ず、個人ＩＤ情報、顔紋情報及び声紋情報を含む登録対象者に関する情報を予め登録した登録データベースを構築し、前記個人ＩＤ情報のうち少なくとも登録対象者固有の識別標識を含む前記登録対象者に関する情報を記憶したＩＣカードを予め発行する。そして前記認証対象者を認証する際に、該認証対象者の顔画像を収録しその顔画像から顔紋情報を抽出すると共に、前記認証対象者が保持する前記ＩＣカードから前記識別標識を読み取る。読み取った識別標識を用いて前記登録データベース内の該当する登録対象者の情報へアクセスし、アクセスした登録対象者の顔紋情報と前記認証対象者の顔紋情報とを比較しその適合率を算出し、該適合率が顔紋情報に係る閾値以上である場合は、該認証対象者が該登録対象者であると判定する。さらに、前記適合率が顔紋情報に係る閾値に達しない場合は、前記認証対象者が自己の個人ＩＤ情報を発声した音声から声紋情報を抽出し、前記認証対象者の声紋情報と、前記読み取った識別標識に該当する前記登録対象者の声紋情報とを比較しその適合率を算出し、該声紋情報の適合率が声紋情報に係る閾値以上である場合は、前記認証対象者が該登録対象者であると判定する。さらに、前記声紋情報の適合率が声紋情報に係る閾値に達しない場合は、前記顔紋情報の適合率と前記声紋情報に係る適合率とを掛け合わせ、前記掛け合わせた数値が第１の閾値以上である場合は、前記認証対象者が前記登録対象者であると判定する。

【００１０】（４）上記（３）の構成において、前記掛け合わせた数値が前記第１の閾値に達しない場合において、前記認証対象者が発声した自己の個人ＩＤ情報と、前記読み取った識別標識に該当する前記登録対象者の個人ＩＤ情報とが一致し、かつ、前記登録対象者について前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第２の閾値以上であるときは、前記認証対象者が前記登録対象者であると判定する。

【００１１】（５）上記（３）の構成において、前記掛け合わせた数値が前記第１の閾値に達しない場合において、前記認証対象者が発声した自己の個人ＩＤ情報と、前記読み取った識別標識に該当する前記登録対象者の個人ＩＤ情報とが一致するが、前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第２の閾値に達しないとき、前記認証対象者の前記ＩＣカードに記憶された暗証番号を読み取り、該読み取られた暗証番号と前記認証対象者が入力した暗証番号とが一致し、かつ、前記登録対象者について前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第３の閾値以上であるときは、前記認証対象者を前記登録対象者であると判定する。

【００１２】（６）上記（１）乃至（５）のいずれかの構成において、前記認証対象者が前記登録対象者であると判定されたとき、前記収録された顔画像から抽出された新たな顔紋情報を前記登録データベース内の該登録対象者に関する情報として追加登録する。そして、追加登録された顔紋情報のデータ数が所定数を超える場合は、その中から最も古い顔紋情報を削除する。また、前記認証対象者の顔紋情報と特定の登録対象者の顔紋情報とを比較しその適合率を算出する際に、該特定の登録対象者に係る全ての登録された顔紋情報と比較し、最も高い適合率を該特定の登録対象者についての前記顔紋情報の適合率とする。

【００１３】（７）上記（６）の構成の顔紋情報を声紋情報に置き換えた構成も可能である。

【００１４】（８）本発明の生態情報による本人認証システムのさらに別の構成においては、先ず、個人ＩＤ情報、顔紋情報及び声紋情報を含む情報を記憶したＩＣカードを予め発行する。そして前記認証対象者を認証する際に、該認証対象者の保持するＩＣカードに記憶された情報を読み取り、前記認証対象者の顔画像を収録しその顔画像から顔紋情報を抽出し、抽出された顔紋情報と前記ＩＣカードから読み取った顔紋情報とを比較しその適合率を算出し、前記適合率が顔紋情報に係る閾値以上である場合に前記認証対象者が本人であると判定する。さらに、前記顔紋情報の適合率が前記顔紋情報に係る閾値に達しない場合、前記認証対象者が自己の個人ＩＤ情報を発声した音声から声紋情報を抽出し、抽出された声紋情報と前記ＩＣカードから読み取った声紋情報とを比較しその適合率を算出し、前記適合率が声紋情報に係る閾値以上である場合に前記認証対象者が本人であると判定する。さらに、前記声紋情報の適合率が、前記声紋情報に係る閾値に達しない場合、前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせ、前記掛け合わせた数値が第１の閾値以上である場合に前記認証対象者を本人であると判定する。

【００１５】（９）上記（８）の構成において、前記掛け合わされた数値が前記第１の閾値に達しない場合に、前記認証対象者が発声した自己の個人ＩＤ情報と前記ＩＣカードから読み取った個人ＩＤ情報とが一致し、かつ前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第２の閾値以上である場合に前記認証対象者を本人であると判定する。

【００１６】（１０）上記（８）の構成において、前記掛け合わされた数値が前記第１の閾値に達しない場合に、前記認証対象者が発声した自己の個人ＩＤ情報と前記ＩＣカードから読み取った個人ＩＤ情報とが一致するが、前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第２の閾値に達しないとき、前記認証対象者のＩＣカードの暗証番号を読み取り、該

読み取られた暗証番号と前記認証対象者が入力した暗証番号とが一致し、かつ、前記顔紋情報に係る適合率と前記声紋情報に係る適合率を掛け合わせた数値が第３の閾値以上である場合に前記認証対象者を本人であると判定する。

【００１７】（１１）本発明の生態情報による本人認証システムのさらに別の構成においては、施設等の内部に滞在している人を管理する在籍管理システムを設け、前記施設等へ入場する際に入場者が本人であると判定された場合に前記在籍管理システムに対してその入場の情報を渡し、かつ、該入場者が退場する際に本人であると判定された場合に該在籍管理システムに対してその退場の情報を渡す。

【００１８】（１２）本発明の生態情報による本人認証システムのさらに別の構成においては、先ず、顔紋情報を含む登録対象者に関する情報を予め登録した登録データベースを構築する。そして前記認証対象者を認証する際に、ビデオカメラにより撮影された映像から該認証対象者の顔画像を収録しその顔画像から顔紋情報を抽出し、抽出された顔紋情報と前記登録データベースに登録された前記顔紋情報とを比較しその適合率を算出し、前記適合率が顔紋情報に係る閾値以上である登録対象者が一人のみの場合に前記認証対象者が該登録対象者であると判定する。さらに、前記ビデオカメラにより撮影された映像上の前記認識対象者の顔画像に重ねて認証済みを示す標識を付す。好適には、前記認証済みを示す標識が、前記登録データベースから取得した前記認証対象者の氏名である。前記適合率が前記顔紋情報に係る閾値に達しない場合には、前記ビデオカメラにより撮影された映像上の前記認識対象者の顔画像に重ねて認証不可を示す標識を付す。好適には、前記認証不可を示す標識が、前記認証対象者の顔画像をプリンキングさせることである。

【００１９】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。本発明による生態情報を利用した本人認証システムは、基本的に顔紋及び声紋の生態情報を利用し、併せてＩＣカードを用いる場合もある。ここで、顔紋とは、本人の顔の形態の特徴的要素であり、指紋や声紋に合わせた用語である。顔紋及び声紋もまた指紋と同様に、本人確認する上で極めて固有性の高い情報の一つである。

【００２０】図１は、本発明による生態情報を利用した本人認証システムにおいて、実際の運用に先立って行われる登録処理１００を概略的に示す流れ図である。特定の施設への入退場する資格を有する入退場者は、予め本人確認用のデータを登録する。登録対象者は、例えば、大学や企業において長期の入退場者となる学生や社員、出入り業者や顧客等の一時的な来訪者である。登録されるデータは、少なくとも個人ＩＤ情報、顔画像情報及び声紋情報を含む。

【００２１】ステップ１０１において、個人ＩＤ情報を登録する。個人ＩＤ情報は、本人の氏名、生年月日、住所等の個人的な情報である。これらに加えて個人ＩＤ情報には、学生番号、社員番号若しくは登録番号等、その組織内における登録対象者固有の識別標識も含まれる。すでにその組織内にこれらの個人ＩＤ情報を格納したデータベースがあれば、その中から必要な事項を取り出すことにより容易に取得できる。登録対象者が、自ら入力してもよい。

【００２２】ステップ１０２において、顔画像情報を登録する。顔画像情報は、登録用カメラの前で静止画像を撮影する。例えば、正面と両斜め２枚の合計３枚等の複数枚を撮影し、これらの画像データを登録する。３方向から撮影するのは、実用時に実際の本人確認を行う際には動画を認識しなければならないため、認証スピードを上げるためである。さらに、撮影された顔画像から顔画像情報すなわち顔紋を抽出する。これは、顔のうちで長期間にも変化の少ない部位の特徴を数値化し、それらの数値データを登録することである。もちろん、顔画像自体も画像データとして登録する。

【００２３】また、顔画像情報の登録の際にも本人の確認を行うことが好ましい。これは、登録時に他人の顔が登録されることを防ぐためである。具体的に例えば、入社時、入学時の願書等に貼付の写真で確認する。

【００２４】ステップ１０３において、声紋情報を登録する。例えば、本人がその氏名や住所等を１０秒間程度発声し、その声を収録する。声紋もまた数値化して数値データとして登録する。

【００２５】以上の登録データは、所定の場所に保存される。基本的形態では、本人認証システムの登録データベースにマスタデータとして保存される。さらに、登録対象者に発行されるＩＣカード内に保存される。ＩＣカードは、ＩＣチップを内蔵したカードであり大容量の情報を記憶することができる。後述するように、非接触で読み取り書き込み可能な非接触型ＩＣカードであることが好適であるが、接触型であってもよい。

【００２６】本人に発行されるＩＣカードにのみデータを保存する実施形態も可能である。その場合はデータベースへのアクセスなしに、入退場するその場で本人認証できるメリットがある。しかしながら、現実的には登録データベースを構築することが望ましい。登録データベースを設けないとすると、声や顔の経時変化や退職して入場不可になった情報等の更新の実行が困難となるためである。

【００２７】ステップ１０４において、登録対象者にＩＣカードが発行される。例えば、そのＩＣカードの表面に顔画像及び個人ＩＤ情報を印刷してもよい。これにより、従来の学生証や社員証と同様にＩＣカードを利用することができる。こうしてステップ１０５において、登

録が完了する。

【００２８】尚、上記のように登録されたデータは、所定の期間毎に更新されることが好ましい。例えば、年に一回更新を行い、ＩＣカードを再発行する。これは、顔紋情報等が経年変化するので、認証率を上げるために行う。あるいは、本人認証システムを実行する過程において本人の顔画像を採取するので、随時、採取された顔画像に基づいて登録データを修正してもよい。

【００２９】次に図２を参照して、本発明による生態情報を利用した本人認証システム２００の第１の形態を説明する。図２は、本人認証システム２００の概略的流れ図である。ステップ２０１において、本人認証システムが、施設等の出入口に接近した人あるいは出入口を通過しようとする人を認知する。すなわち、本システムを適用すべき認証対象者を特定する。特定方法は、以下の通り、種々可能である。

【００３０】例えば、認証対象者が非接触型ＩＣカードを携帯している場合、システムがＩＣカードに電波を当てることによりＩＣカードの存在を検知することができる。これにより、システムは認証対象者が出入口に近付きつつあることを認知する。あるいは、非接触形ＩＣカードに適さない環境においては、例えば病院等において電波授受が好ましくない場合、接触型ＩＣカードをＩＣカードリーダに読み取らせることで認証対象者の存在を本システムが認知してもよい。さらにまた、入退場者がＩＣカードを携帯していない場合は、出入口への接近者の存在を感知するセンサ等により、あるいは認証対象者自身が出入りしたい意思を示す操作（操作パネルやドアホンのボタンを押す等）を行ったりすることで、本システムが認証対象者の存在を認知してもよい。

【００３１】そして、指定した場所において認証対象者がカメラの方を向いた場合に、システムはその人が認証対象者であると判断する。指定した場所でカメラを向くことは、予め認証対象者に了承させてもよく、その場所に標示してもよく、あるいは好適には、認証対象者が意識せずとも自然な形でカメラの撮影可能な場所に立つことになるような設計としてもよい。認証対象者でない人すなわち登録データの無い人は、たとえカメラの方を向いても除外されるので問題はない。

【００３２】ステップ２０２において顔画像の収録を行う。例えば、非接触型ＩＣカードを携帯している場合は、対象者が携帯しているＩＣードを読み取ったときに電波により距離を計算して撮影する。電波で距離を測定し、認証対象者が撮影時点を通過するときを予測して撮影する。また、別の収録方法としては、動いてくる人をカメラで追跡し、焦点距離を合わせた時点を通過する時に撮影する。あるいは、マンションの玄関等の場合は、インターフォンの前に認証対象者が立った時点で撮影してもよい。いずれにしても対象者の位置を感知するセンサを利用する。

【００３３】ここで、正面画像の採取について説明する。基本的には認証対象者が顔画像を採取することを認識しているので、撮影に適した方向からカメラの方を向くことは期待できる。逆に、認識していない人はカメラの方を向かないので、それにより対象者から除外することもできる。あるいは、カメラの方を向くように文字や音声の案内で促してもよい。一般的に、正面を向かせることが難しいことも多いので、斜めの顔を左右の眼球位置を使って回転させて正面画像に補正して顔紋情報を正確に取れるようにする。

【００３４】次に、ステップ２０３において、顔画像情報の抽出を行う。上記の登録時の顔画像情報の抽出と同じ手法を用いて顔紋を数値化する。例えば、左右の眼球の距離、鼻、口との距離等少なくとも２０箇所以上の数値を用いることが好適である。尤も、登録時は正面で焦点も合っているが、実際の運用時には動画像であるため外乱が予想されるので適宜補正する。

【００３５】その後、ステップ２０４において、顔認識システムを用いて本人認証を実行する。先ず、認証対象者のＩＣカードに保存された個人ＩＤ情報のうち学生番号または社員番号等の識別標識を読み取り、この識別標識に該当する登録データベース内の登録対象者の情報にアクセスする。該当する登録対象者の登録された顔紋情報と、ステップ２０３で抽出された顔紋情報とを比較する。双方とも数値情報であるので統計的に比較し、適合率を算出することができる。そしてステップ２０５において、算出された適合率が閾値以上であるか否かを判定する。閾値は、保安管理の必要性等に応じて適宜設定することができ、例えば「９９．０％」等である。閾値以上であれば認証対象者がその登録対象者である、すなわち本人であると判定する。このように登録データベース内の特定の登録対象者へアクセスすることは、登録データベース内の全登録対象者を走査するよりも遙かに短時間で実行できるため、効率的である。

【００３６】一方、ステップ２０１において認証対象者がＩＣカードを携帯していない場合におけるステップ２０４の顔認識システムによる本人認証は、登録データベースの保存情報へのアクセスにより実行される。この場合、前述の通り、認証対象者の存在をＩＣカード以外の任意の方法で検知して特定し、上記ステップ２０２及び２０３と同様に顔画像の収録及び顔紋情報の抽出を行う。そして、ステップ２０４において、上記の登録データベース内の全登録対象者の顔紋情報を参照して、採取した顔紋情報との適合率が閾値以上の人をリストアップする。そしてステップ２０５において、リストアップされた人が一人のみであれば、認証対象者がその登録対象者である、すなわち本人であると判定する。

【００３７】ステップ２０５において本人であると判定されたならば、ステップ２１３において、必要に応じて今回の認証実行記録に基づきデータベース内の本人情報

を更新するようにしてもよい。ステップ２１３のデータベース更新方法の簡単な例としては、ステップ２０３で抽出された顔紋情報を新たな顔紋情報としてデータベースに再登録する方法がある。

【００３８】ステップ２１３における顔紋情報の更新すなわち再登録を行う好適例について説明する。先ず、登録データベース内に一人の登録対象者についての顔紋情報のデータを複数個格納できるようにする。そして、認証対象者が入退場する毎に抽出される新たな顔紋情報を順次それらの複数の格納場所に追加登録していき、格納場所の数を超える新たな顔紋情報を追加登録しようとする場合には、最も古い顔紋情報を削除する。この好適例の場合においては、上記のステップ２０４で登録データベース内の顔紋情報と比較する際に、これら複数の格納された顔紋情報の各々と比較して複数の適合率を算出し、最も高い適合率をその登録対象者の顔紋情報の適合率として採用する。

【００３９】後述する声紋情報についても、全く同様の方法で一人の登録対象者について複数の声紋情報を登録データベース内に格納しておき、声紋情報の比較のために利用することができる。

【００４０】この好適例の方法よれば、顔紋情報や声紋情報という生態情報がその日の体調等により変化したり、長期的に変化したりする場合であっても常に的確な認証を行うことができる。

【００４１】その後、ステップ２１４において終了する。ステップ２１４においては、認証を終了した旨を表示するかあるいは出入口のロック解除を行う等して、対象者に認証されたことを示す。

【００４２】ステップ２０５において閾値以上の適合率が得られなかったか、あるいは、リストアップされた人が一人のみでなかった（零または複数）等の理由により、個人特定ができなかったならば、ステップ２０６において、認証対象者に対して個人ＩＤ情報を発声することを求める。このとき、システムが音声により質問をしてもよく、あるいは質問を画面表示してもよい。質問される個人ＩＤ情報は、氏名または生年月日等であり、認証対象者が本人と確認されるまで質問を繰り返す。声紋を採取することが主目的であるので、同一の質問を繰り返す方法でもよい。ステップ２０７において、認証対象者は、質問に対して音声により回答し、システムはこの音声を収録する。ステップ２０６及び２０７における個人ＩＤ情報に関する質問及び音声収録は、認証対象者から声紋を採取することが第１の目的であるが、後の認証ステップのために認証対象者自身から個人ＩＤ情報を取得することが第２の目的である。

【００４３】ステップ２０８において、収録した音声から音声認識システムを用いて声紋を採取し、それを数値化する。そしてステップ２０９において、数値化された声紋を登録データベースに保存された声紋データと比較する。先のステップ２０４でＩＣカードから識別標識を読み取っている場合は、該当する登録対象者の声紋データにアクセスし、これと比較する。

【００４４】一方、ＩＣカードを携帯していない場合は、最初に行った顔紋情報の適合率が閾値には到達しなかったが最も高かった登録対象者の声紋データにアクセスし、これと比較することが好適である。データベース中の特定の登録対象者のデータにアクセスすることは、データベース全体を走査するよりも遙かに短時間でできき、効率的だからである。これらの比較の結果、同一人と判定できる程度の声紋の適合率が得られたならば、本人であると判定し、ステップ２１３を経てステップ２１４で終了する。

【００４５】ＩＣカードを携帯していない場合において、上記の特定の登録対象者の声紋データとの比較の結果、同一人であるとの判定ができないときは、データベース全体を走査して適合率の高い人をリストアップする。その結果、声紋における適合率の所定の閾値以上の適合率をもつ人が一人であれば、本人と判定し、ステップ２１３を経てステップ２１４で終了する。

【００４６】さらに、声紋に関してリストアップされた人の適合率がいずれも所定の閾値に達しなかったか、あるいは、リストアップされた人が一人のみでなかった等の理由により、声紋認識のみでは個人特定できなかった場合は、最初に行った顔紋情報に関する適合率によりリストアップされた人と共通する人について、顔紋情報と声紋の双方の適合率を掛け合わせる。掛け合わせの結果、得られた数値が所定の閾値以上の人が一人であれば、本人であると判定する。

【００４７】単独の適合率同士を掛け合わせる計算の具体例は以下の通りである。R1を顔紋の適合率、R2を声紋の適合率とすると、掛け合わせた適合率は、1－(1－R1)＊(1－R2)となる。例えば、顔紋情報の適合率の閾値が９０％(R1=0.90)であり、かつ、声紋の適合率が９４％(R2=0.94)である人の場合、これらを掛け合わせた適合率は、1－(1－0.90)＊(1－0.94)=0.994という数値が得られ、９９．４％となる。

【００４８】ここで、顔紋情報と声紋の双方の適合率を掛け合わせた数値の閾値が、９９％と設定されているならば、この人の数値は９９．４％で閾値以上であるので、他にこの閾値以上の数値を示す人が抽出されなければ、本人と判定し、ステップ２１３を経てステップ２１４で終了する。

【００４９】本明細書中では、便宜上、顔紋情報と声紋の双方の適合率を掛け合わせた数値を単独の適合率と区別するために「適合度」と称し、適合度を評価するための閾値を他の閾値と区別するため、「第１の閾値」と称する場合がある。

【００５０】ステップ２０９において、声紋の適合率と顔紋情報の適合率を掛け合わせた適合度の評価によって

も個人特定ができない場合は、ステップ２１０へ進む。ステップ２１０では、ステップ２０７で収録した音声から、個人ＩＤ情報の内容を取得する。そして、ステップ２１１において、データベースに登録された個人ＩＤ情報と比較する。そして、個人ＩＤ情報が一致すれば、その人の顔紋情報適合率及び声紋適合率を掛け合わせた適合度を加味して、所定の閾値以上であれば、本人であると判定する。個人ＩＤ情報の一致のみでは、他人のなりすましを排除できないためである。この時点では、個人ＩＤ情報の一致という要素が加わるので、適合度の閾値を、上記の第１の閾値９９．０％よりも低くすることができる。例えば、閾値を８５．０％とすると、適合度８８．０％を示す人が一人であれば、本人と判定する。そしてステップ２１３を経てステップ２１４で終了する。

【００５１】本明細書中では、顔紋情報と声紋の双方の適合率を掛け合わせた適合度と個人ＩＤ情報とを併せて評価するための閾値を、便宜上「第２の閾値」と称する場合がある。

【００５２】ステップ２１１において、顔紋情報と声紋の双方の適合率を掛け合わせた適合度と個人ＩＤ情報とを併せた評価によっても個人特定できない場合において、認証対象者がＩＣカードを携帯していないとき及びＩＣカードの携帯を前提としないシステムでは、ここでこの認証対象者の出入口の通過は拒否される。

【００５３】一方、ＩＣカードを携帯している場合は、ステップ２１２へ進む。ステップ２１２において、認証対象者が携帯しているＩＣカードの内容を読み込み、ＩＣカードによる認識システムを実行する。具体的には、ＩＣカード認識システムが、ＩＣカードに記憶された暗唱番号若しくは識別コード等の本人のみが認知している情報を読み込んだ後、認証対象者に対しその暗証番号等を入力するように求める。この入力操作を行うためにキーボードやタッチスクリーン等の入力手段が設けられている。そして、ＩＣカードの記憶内容と認証対象者の入力内容が一致したならば、既に得られている顔紋情報適合率及び声紋適合率を掛け合わせた適合度を加味して、所定の閾値以上であれば本人であると判定する。ＩＣカード内容の一致のみでは、他人のなりすましを排除できないためである。この時点で、この認証対象者は、ステップ２１１における個人ＩＤ情報の一致及びこのステップにおけるＩＣード内容の一致という要素が加わっているので、適合度の閾値をステップ２１１の第２の閾値８５．０％よりもさらに低くすることができる。例えば、閾値を８０％とすると、適合度８２％を示す人が一人であれば、本人と判定する。そしてステップ２１３を経てステップ２１４で終了する。

【００５４】本明細書中では、顔紋情報と声紋の双方の適合率を掛け合わせた適合度とＩＣカード内容（個人ＩＤ情報の一致は既に確認済み）とを併せて評価するための閾値を、便宜上「第３の閾値」と称する場合がある。

【００５５】尚、ステップ２１２におけるＩＣカードによる認識システムによっても個人特定できなかった場合は、その認証対象者の出入口の通過は拒否される。

【００５６】図２の本人認証システムにおいては、顔紋情報、声紋、個人ＩＤ情報、ＩＣカード内容に基づき、順次認証を実行していき、途中のステップで十分に本人認証がなされたと判定されたならば、以降のステップを省略する。尚、上記の例では、顔紋情報と声紋を加味して考慮する方法として適合率の数値を掛け合わせたが、他の方法によって行ってもよい。例えば、顔紋情報及び声紋情報の適合率並びに個人ＩＤ情報及びＩＣカード内容の一致を適宜のポイントに換算して足し合わせ、所定の閾値ポイントに達した時点で本人と判定し、認証システムを終了するという方法も可能である。あるいは、適合率の数値をそのまま掛け合わせるのではなく、適宜の重みを付けた上で掛け合わせてもよい。このように、顔紋情報及び声紋の適合率の双方を加味して本人認証を行うための任意の方法は、全て本発明に含まれるものとする。さらに、顔紋情報及び声紋情報を利用した本発明の方法に加えて、指紋若しくは虹彩等の他の生態情報による認識システムを併用した方法もまた、本発明に含まれるものとする。

【００５７】図２に示した本人認証システムは、例えば、セキュリティを保つ必要のある事務所の入退室管理、放射線関連の施設の入退室管理に好適であるが、安価に構成することにより民間の住宅にも適用可能である。

【００５８】図３は、本発明による生態情報を利用した本人認証システムの第２の実施形態３００を示す概略的流れ図である。これは、認証対象者がＩＣカードを保持していることを前提としたシステムである。

【００５９】先ずステップ３０１において、認証対象者が出入口に近付き、ＩＣードの読み取り可能範囲に入ってきたとき、その人の保持しているＩＣカードの記憶内容を読み込む。読み込みデータには、顔紋情報、声紋、個人ＩＤ情報、暗唱番号等が含まれる。本実施形態では、基本的にＩＣカードに記憶されたデータと認証対象者自身とを比較することにより本人認証を行う。

【００６０】尚、認証対象者がＩＣカードを忘れてきた場合でも対応できるように、ステップ３０２において認証対象者が登録番号等を入力することにより、次のステップへ進めるようにしてもよい。ステップ３０２を経た場合は、入力された登録番号に対応する登録データベース内のデータと認証対象者自身とを比較することにより本人認証を行うこととなる。従って、ステップ３０２で入力する登録番号は、暗証番号の意味ではなく、登録データベース内の特定の人のデータを指定するためのものである。以下、説明を簡便とするために、ステップ３０２を経て本人認証を行う場合については省略するが、「ＩＣカード内に記憶されたデータ」を「入力された登

録番号により指定された登録データベース内の個人データ」と読み替えればよい。

【００６１】ステップ３０３において認証対象者の顔画像を収録し、ステップ３０４において、収録された顔画像から顔紋情報を抽出する。これらのステップ３０３及び３０４は、図２のステップ２０２及び２０３と同様である。

【００６２】ステップ３０５において、顔認識システムを用いてステップ３０４で取得した顔紋情報とＩＣカードから読み取った顔紋情報とを比較し適合率を算出する。これは、図２のステップ２０４においてＩＣカードから読み取った顔紋情報と比較する場合と同様である。さらにステップ３０６において、算出された適合率が所定の閾値以上であるか否かを判定する。所定の閾値以上の適合率であれば本人と特定する。そして、ステップ３１４で、登録データベースの本人情報を必要に応じて更新し、ステップ３１５で終了する。ステップ３１４及び３１５は、図２のステップ２１３及び ２１４と同様である。

【００６３】ステップ３０６において閾値以上の適合率が得られなかったならば、ステップ３０７において、認証対象者に対して個人ＩＤ情報を発声することを求める。ステップ３０８において、認証対象者は、質問に対して音声により回答し、システムはこの音声を収録する。ステップ３０９において、収録した音声から音声認識システムを用いて声紋を採取し、それを数値化する。ステップ３０７～３０９は、図２の２０６～２０８と同様である。

【００６４】そしてステップ３１０において、数値化された声紋を、ステップ３０１でＩＣカードから読み取った声紋データと比較する。この結果、同一人と判定できる程度の声紋の適合率が得られたならば、本人であると判定し、ステップ３１４経てステップ３１５で終了する。

【００６５】声紋データのみでは、同一人との判定ができない場合は、最初に行った顔紋情報に関する適合率と声紋に関するそれとを掛け合わせる。掛け合わせの結果、得られた数値が所定の閾値以上であれば、本人であると判定する。適合率の掛け合わせによる判定方法は、図２で説明した通りである。本人と判定されたならば、ステップ３１４を経てステップ３１５で終了する。

【００６６】ステップ３１０において、声紋の適合率と顔紋情報の適合率を掛け合わせても、適合度が閾値以上とならなかった場合は、ステップ３１１へ進み、ステップ３０８で収録した音声から、個人ＩＤ情報の内容を取得する。そして、ステップ３１２において、ＩＣカードから読み取った個人ＩＤ情報と比較する。そして、個人ＩＤ情報が一致したならば、その人の顔紋情報適合率及び声紋適合率を掛け合わせた適合度を加味し、所定の閾値以上であれば、本人であると判定する。個人ＩＤ情報の一致のみでは、他人のなりすましを排除できないためである。この時点では、個人ＩＤ情報の一致という要素が加わるので、適合度の閾値をステップ３１０の閾値よりも低くすることができる。これは、図２のステップ２１１での説明と同様である。本人と判定されたならば、ステップ３１４を経てステップ３１５で終了する。

【００６７】ステップ３１２においても本人と特定できない場合は、ステップ３１３へ進む。ステップ３１３において、ステップ３０１で読み取ったＩＣカード内の暗証番号による認識システムを実行する。具体的には、認証対象者に対し暗証番号を入力するように求める。そして、ＩＣカード内に記憶された暗証番号と認証対象者の入力内容が一致したならば、既に得られている顔紋情報適合率及び声紋適合率を掛け合わせた適合度を加味して、所定の閾値以上であれば本人であると判定する。暗証番号の一致のみでは、他人のなりすましを排除できないためである。この時点で、この認証対象者は、ステップ３１２における個人ＩＤ情報の一致及びこのステップにおける暗証番号の一致という要素が加わっているので、適合度の閾値をステップ３１２の閾値よりもさらに低くすることができる。本人と特定されれば、ステップ３１４を経てステップ３１５で終了する。

【００６８】尚、ステップ３１３に至った時点で、ＩＣカードを保持していない認証対象者は、入退場を拒否される。また、ステップ３１３におけるＩＣカードによる認識システムによっても本人と特定できなかった場合も、その認証対象者の入退場は拒否される。

【００６９】図３に示した本人認証システムは、大学等の学生証をＩＣカードとし学生の大学への立入りを管理する場合に好適である。また、事務所や病院等の職員の身分証明書をＩＣカードとし、あるいは、フィットネスクラブ等の会員証をＩＣカードとしても好適である。大学等の出席管理に適用し、「単位」認定の基礎データとする。

【００７０】図４は、本発明による生態情報を利用した本人認証システムを応用した入退室管理システム４００の概略的流れ図である。このシステムは、建物若しくは部屋への入場チェックを行うと共に、退去確認も行うことにより、建物等の中にいる人を把握したり、夜間等に保安体制を解除する際の無人確認等を行ったりできる。以下の図４の説明では、室内への入退室をイメージして説明するが、部屋に限らず建物であっても同様である。

【００７１】ステップ４０１～４０６は、入室時の処理の流れであり、ステップ４１１～４１６は、退室時の処理の流れである。先ず入室時には、ステップ４０１において入室者の保持するＩＣカードを読み取ることにより少なくとも顔紋情報のデータを取得する。次にステップ４０２において入室者の顔画像を収録し、ステップ４０３において収録した顔画像のデータから顔紋情報を抽出する。ステップ４０４において、抽出した顔紋情報とＩ

Ｃカードから読み取った顔紋情報とを顔認識システムを用いて比較し、適合率を算出する。その後、ステップ４０５において、算出された適合率が所定の閾値以上であるか否かを判定する。所定の閾値以上の適合率であれば本人と特定する。本人と特定されたならば、在室者として在室登録すると共に入室させる。ステップ４０５において、適合率が閾値に到達しなかった場合は、ステップ４０２へ戻り同じ処理を繰り返す。

【００７２】退室時の処理も全く同じである。ステップ４１５において本人と特定されたならば、在室登録を取り消すと共に退室させる。

【００７３】入退室管理システム４００は、在室者に関する在室管理システム４２０の機能も実行する。例えば、現時点での在室者名、人数、在室時間を表示したりする。これにより最終退出者の確認ができ、入り口や玄関をロックすることができる。また、守衛室での最終退室者管理を自動化、確実化できる。

【００７４】尚、図２～図３で説明した各実施形態においても、図４に示したような在室管理システムを設けることができる。入退場する施設等は部屋に限定されないため、広い意味で在籍管理システムと称することとする。すなわち、施設等へ入場する際に入場者が本人であると判定された場合に、在籍管理システムに対してその入場の情報を渡し、かつ、その入場者が退場する際に本人であると判定された場合に、在籍管理システムに対してその退場の情報を渡すようにする。

【００７５】またさらに、広い建物や会場においては、複数のＩＣカード読取装置あるいはカメラ等をセットした本人認証装置を随所（例えば、建物内の各部屋）に設置することにより、部屋別在室者を把握することができる。

【００７６】以上説明した各実施形態において、その実行の結果、認証対象者の出入口の通過が拒否された場合、その後の対応を守衛等の管理者の判断に委ねてもよい。いずれにしても、本システムを利用することにより、人手によるチェック該当者を絞ることができるためコストを下げることができる。

【００７７】図５は、本発明の生態情報による本人認証システムを応用した集中監視システム５００の概略的流れ図である。出入り口の多い施設では、入場管理を徹底するのは困難であり、システム化で無人化することも困難である。出入り口の多い施設では、保安室（管理センター）で集中管理する必要がある。

【００７８】大きな工場や大学のように建物に出入り口が多くあり、常時多くの人が出入りする場合、ビデオ監視システムがよく用いられている。ビデオ監視システムでは、各出入り口にビデオカメラを設置し、映像を管理センターへ送り、管理センターでは複数の画面に映し出される映像を保安担当者が監視する。

【００７９】先ず、ステップ５０１において監視用ビデオカメラの映像から顔画像を収録する。ビデオカメラには複数の人が移っている場合があるが、一人一人順次認証していく。収録された顔画像から、ステップ５０２において顔紋情報を抽出する。そして、抽出された顔紋情報を、ステップ５０３において登録データベース内に格納された顔紋情報データと比較することにより適合率を算出し、ステップ５０４におい入場者が誰であるかを個人特定する。個人特定された人は、ステップ５０８においてそのまま入り口を通過する。

【００８０】好適例では、個人特定された人については、ビデオカメラ映像中のその人の映像に対しその氏名を重ねて書き込み認証済みであることを保安担当者に対して示す。

【００８１】ステップ５０４において個人特定できなかった人については、ステップ５０５において管理センターに送信されたビデオ映像中のその人の映像をブリンキング（点滅処理）等させて注意を保安担当者に注意を促す。

【００８２】ステップ５０６において、保安担当者が映像中でブリンキングされた人の顔画像を目視確認する等して不審者か否かをチェックする。そしてステップ５０７において所定の入場手続を経る等して、その人の入場を許可する。

【００８３】

【発明の効果】以上述べた通り、本発明は、本人認証を行うために顔紋、声紋、ＩＣカードを利用し、かつ、これらの手法を必要に応じて併用することにより、個々の手法のみによる識別力の不備を補充し、実用に耐え得る本人認証システムを実現した。本発明のシステムは、個々の認証手法の単なる組み合わせではなく、それ以上の効果を発揮する。なぜなら、各認証ステップを順次行っていく途中で十分な認証が得られた場合は、以降のステップを省略して本人認証を終えることにより、極めて効率的に短時間で実行されるからである。さらに、本発明では、顔画像を収録する際、認証対象者が普通に歩いたり、立ったり、カメラの方を向く等の無理のない自然な動作を行っているときに撮影するので対象者に負担を感じさせず、手間も取らせない。また、基本的に無人で入場管理することができ、守衛やガードマン等の人件費を節約できると共に、導入及び維持が容易でかつ費用が安価である。さらに、安価と簡便さが達成できることにより、事務所やマンションばかりでなく、各家庭にも気軽に設置でき、社会環境の悪化に対応できる快適な住生活を営むことができる。

【図面の簡単な説明】

【図１】本発明による生態情報を利用した本人認証システムのために予め行われる本人情報登録処理の概略的流れ図である。

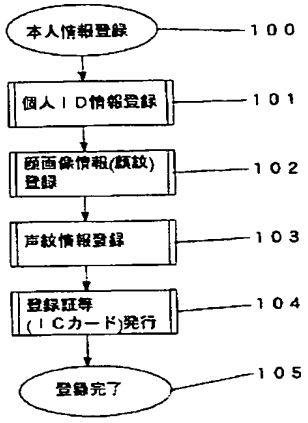
【図２】本発明による生態情報を利用した本人認証システムの一実施形態の概略的流れ図である。

【図３】本発明による生態情報を利用した本人認証システムの別の実施形態の概略的流れ図である。

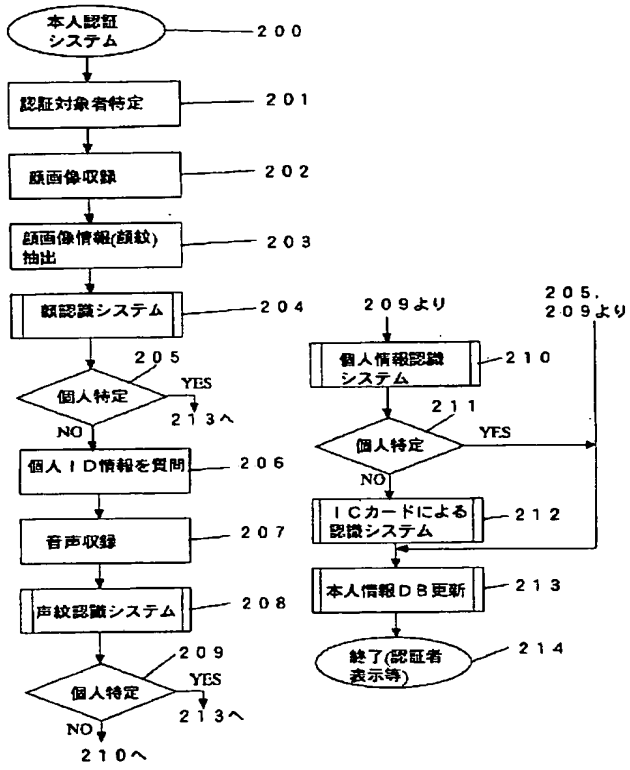
【図４】本発明による生態情報を利用した本人認証システムを応用した入退室管理システムの概略的流れ図である。

【図５】本発明による生態情報を利用した本人認証システムを応用した集中監視システムの概略的流れ図である。

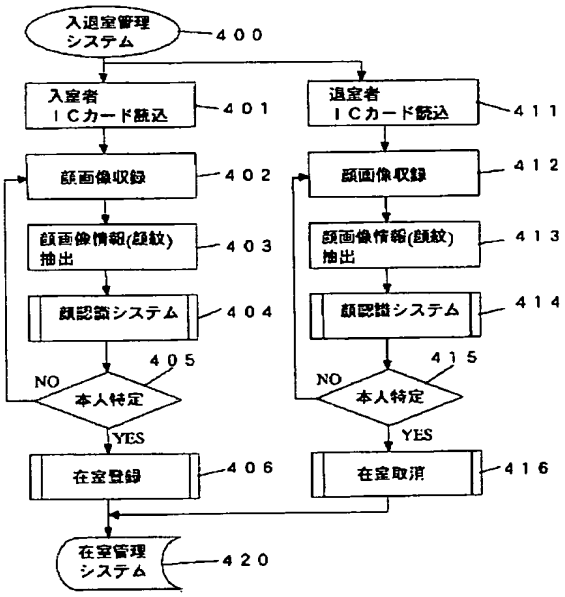
【図１】



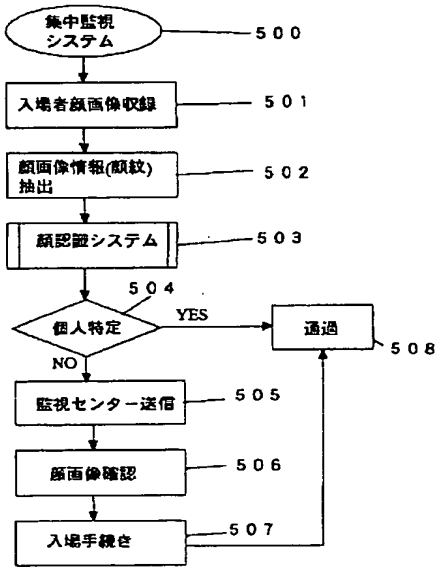
【図２】



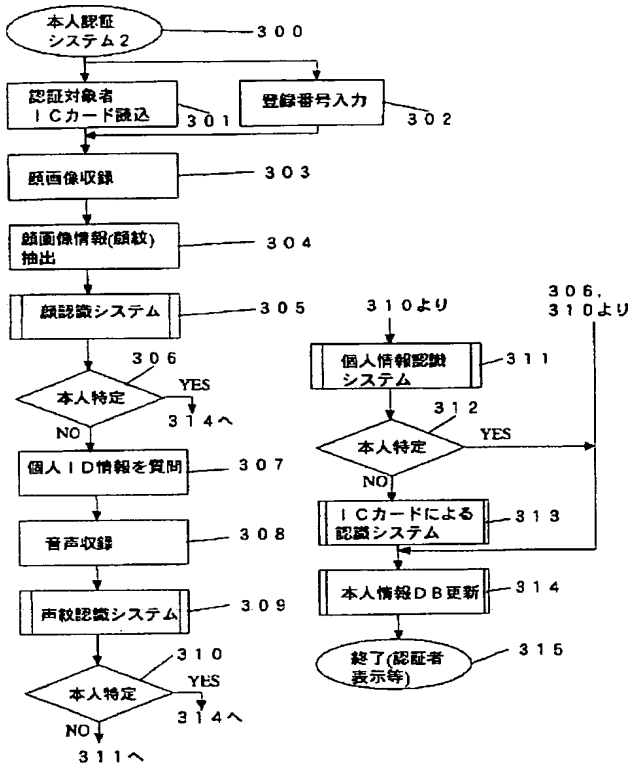
【図４】



【図５】



【図３】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ１０Ｌ 15/28		Ｇ１０Ｌ 3/00	５４５Ｄ	
Ｈ０４Ｎ 7/18			５５１Ｓ	

Ｆターム(参考) 5B035 AA13 BB09 BC01 CA23
5B043 AA04 BA01 BA04 DA05 FA04
GA01 GA13 GA18 HA02 HA05
HA15
5B058 CA15 KA01 KA11 KA33 KA37
KA38 YA11 YA18
5C054 AA04 DA01 EA05 FC12 GA04
GB12 HA18
5D015 AA04 AA06 BB01 GG04 KK02